Protecting and Strengthening Societies

Author
Jeff Frazier

July 2007

Cisco Internet Business Solutions Group (IBSG)

Protecting and Strengthening Societies

Before their arrests for the "Beltway sniper" attacks, which occurred in the mid-Atlantic United States in 2002, the license plate of the car driven by John Allen Muhammad and Lee Boyd Malvo was, in the space of a month, spotted and queried by different U.S. police organizations on 13 separate occasions. But the individual officers running checks on the car had no idea that other police agencies also were on the lookout for the snipers.

If technology had been used to gather information from other jurisdictional sources, that information would have revealed more details such as the number of license plate queries made by other police agencies. Knowing this may have expedited the search.

Using technology in this way would also have benefited police in the 2004 Madrid train bombings. The primary suspect, Jamal Zougam, had been tracked and followed by five different crime and intelligence agencies since 2001. He was finally detained two days after the attack.

In both examples, the agencies' access to information stopped in line with their jurisdictional boundaries. Information did not become knowledge because it was not shared across those lines.

Government is moving into the information age, but not fast enough. Effective government is faced with a 21st-century governance paradox—minimizing the complexity of administrative protocols to determine who is responsible for what. How, to whom, when, and where information is available can fundamentally influence the success or failure of public institutions charged with safeguarding communities. The need to reconfigure how information is created and disseminated is critical in the face of a whole new world of threat. This need is what Sir Ian Blair, London's metropolitan police commissioner, refers to as the "new normality," which describes the tremendous rise in nonroutine problems, such as terrorism and non-natural disasters, that threaten every society.

Senator Richard Shelby, former vice chairman of the U.S. Senate Select Committee on Intelligence, made a similar argument in his investigative report on the September 11 terrorist attacks. Shelby pointed out that all the missed, or misinterpreted, signals (information) that led up to the attack were not shared among the CIA, FBI, or the National Security Council. The information was there, but U.S. intelligence agencies were unable to "connect the dots" of information, as Shelby put it, to possibly intercept the attacks.

Traditional Approaches

A number of social scientists and public safety experts have conducted experiments and research to understand how threats against societies begin and escalate. In 1982, James Wilson, Ronald Reagan professor of public policy at Pepperdine University in California and a former chairman of the White House Task Force on Crime, and George Kelling, an adjunct fellow at the Manhattan Institute for Policy Research, developed the "Broken Windows" thesis, which acknowledges the connection between disorder, fear, crime, and urban decay that have plagued communities for decades. The theory behind the thesis is that if you leave a window broken, it will invite more crime.

The Broken Windows thesis was the inspiration for the cleanup of the New York City subway system in the late 1980s and early 1990s. Removing graffiti and cracking down on the people who leaped over turnstiles without paying would solve two "trivial" problems that were thought to encourage more serious crimes. Not only did this strategy work (since 1990, felonies have fallen more than 50 percent), but one of its architects, Chief of Transit Police William Bratton, would later take his ideas about preventing crime to the city when he became commissioner of the New York City Police Department (Bratton is currently chief of the Los Angeles Police Department).

In Bratton's approach to connecting the dots, he used a system called CompStat,[1] which was influenced by Broken Windows. CompStat (short for COMParative STATistics) organizes computer statistics in a particular way to predict and combat crime in communities. This approach is used today by many public safety agencies; it is limited to a community, however, and by the usefulness of the organization and its capacity to share knowledge with other organizations. But what if the problem is larger than a community? What if the problem exists within a region or country?

Nature of Sovereignties

Because the dangers we face today mutate from one place and source to another, the prevalent approach is to address each threat discretely with a separate agency. But the resources available to each agency are finite and subject to increasing demands and competition. Our inability to piece together information hints at the problem of governance—that is, the attitude of government officials/agencies that if the problem is not in their community, it is not their problem.

Although technology can provide a basis for improved interaction among governments and increased citizen engagement, getting it to work in practice depends first on adopting a new mind-set. This can be a challenging prospect for agencies hampered by poor management, siloed cultures, and inadequate communication. Old hierarchies and structures are not flexible enough to predict and respond to threats quickly. These inherent behaviors prevent agencies from operating effectively in the new, information-rich environment.

---

1. www.gladwell.com/2003/2003_03_10_a_dots.html.

Organizations need to change and work with new, emerging models that demonstrate the power of connectivity to turn information into intelligence and make it available where, when, and for whom it is needed. Organizations also must understand how collaboration can traverse traditional boundaries and develop levers for action—both technological and organizational—that will accelerate progress in protecting communities.

Of course, making information available (capturing and sharing what we know) to the right people at the right time is the fundamental basis for strengthening our communities. But the constantly changing nature of threats posed by a multitude of different criminal, terrorist, and natural catastrophes increasingly means that traditional approaches to information gathering and communication are no longer effective. This is especially true when dealing with criminality and terrorism, which operate across borders and through loose coalitions of networked cells and individuals. Hierarchies and control structures have mutated into much looser and disparate matrices and networks.

Effective 21st-century government requires a new approach to "connecting the dots" by coordinating activities across traditional jurisdictional boundaries.

A Shift in Thinking: Power at the Periphery

All information is quickly becoming digital. Take e-commerce, for example; 90 percent of online communications involve connections—connecting people to businesses, businesses to machines, and machines to machines. But, these connections are not enough. It is critical to connect information to people and organizations at the "edge"— those people who are closest to and may have answers to a given problem or risk, such as the policemen in the examples above. The more we connect the right information to the right people at the right time, the smarter we are about anticipating risks, solving problems, and ensuring public safeguards. In other words, it is the "wisdom of the crowd" that has the power to resolve problems and effect change.

The wisdom-of-the-crowd mentality is true not only for human networking, but also for computer communications networks—those that allow several hundred major communications stations to talk to one another, especially prior to and after an enemy attack or natural disaster. Without an increase in the size of agencies or their budgets, it becomes a challenge to transform thinking about strengthening our communities and improving our public safety and security.

Distributing the Power

Social scientists and public safety researchers are taking a new look at this age-old problem. With the evolution of increasingly intelligent networking and developments in next-generation Internet technologies (including Web 2.0), the model for effective public safety and security must shift from centralized, command-and-control networks to shared, relational systems in a distributed framework that comprises "small pieces loosely joined."

This distributed framework was created by Paul Baran, who developed packet-switched networks to provide a communications solution that would withstand a nuclear attack. While this approach was important to the defense strategy of the United States, it later developed into what is known today as the Internet. Baran's theory of connecting the dots in a distributed, horizontal way is the basis for connecting communities, governments, and public safety agencies as never before.

Although there are a wide variety of network configurations, all can be categorized as centralized (star), decentralized (starbursts), or distributed (grid or mesh), as shown in Figure 1.

Figure 1. Network Configurations

Centralized   Decentralized   Distributed
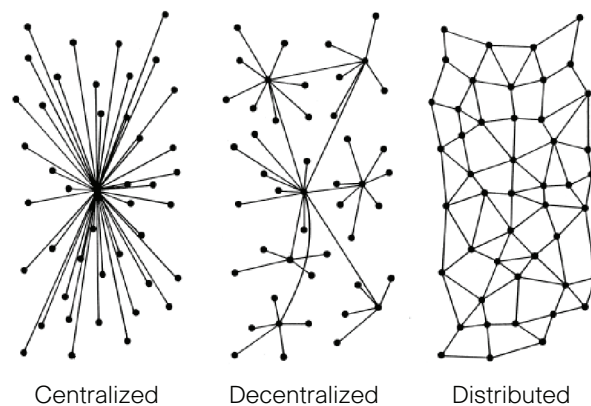
Source: Paul Baran, "On Distributed Communications Series," *Introduction to Distributed Communications Networks* (chapter 1), RAND Corporation, 1964

Unlike centralized and decentralized networks, which are loosely sewn together and open to attacks, distributed networks are strong, tightly sewn, self-supporting infrastructures that enable better collaboration. The value of a distributed environment is that the network learns faster and gathers more intelligence and information than any individual or organization, and shares information with other networks. A distributed network then pushes knowledge to the periphery, or the edge, so that people closest to the problem have the best information to solve the problem. This approach is more resilient and effective than any other.

This new way of thinking seems ideal, but how do we achieve it? We do so by estab-lishing a policy agenda that focuses more on problems than on organizational structure, which is imperative for a knowledge-based organization. Creating such a policy can be achieved easily through Net Learning, an organizational process through which people seek affinity and collateral relationships, and then exercise their influence to share information. Adopting this approach allows organizations to recognize the dangers of overclassifying and compartmentalizing knowledge.

The Right Platform

Before we can create the right distributed communications platform, we must answer two questions: How can we create open standards that allow communities to collaborate? How can we address the growing need for nonhierarchical solutions?

Rather than focusing on specific problems in isolation, looking at them in a distributed manner creates a single, flexible platform that can respond and adapt to a multitude of problems. The basis for this approach is the network or, more specifically, a distributed network that achieves resilience and flexibility by maximizing the ability of agencies and citizens to interact, collaborate, learn, and share information directly with one another. In other words, we need to capture what we know, or don't know; analyze what we know; share what we know; and improve what we know to increase our knowledge about a problem so that we can solve it.

Agencies have vastly improved their ability to gather and use information. The next stage is to pool together all information so that separate pockets of knowledge are connected, rapidly increasing the amount of intelligence that security services can address during a threat.

This approach is starting to emerge in projects such as Intellipedia, established by the Office of the Director of National Intelligence in the United States, using the same technology that powers the online encyclopedia Wikipedia. Intellipedia allows authorized users from 16 government intelligence agencies in the United States to contribute, review, and edit security-related information and build resources and analysis relevant to particular threats. To date, more than 3,600 analysts have contributed more than 28,000 pages. Although there is no public access to the three "wikis" (collaborative software) Intellipedia comprises, it is easy to see how this framework could be adapted to link a wide range of official and public users and sources to build a new and powerful intelligence community.

Additional advances in IP (Internet Protocol) technology mean that investments in older (analog) communications equipment for voice, video, and data can be converted into digital assets that use an existing platform based on Internet technology. These advances are critical for leaders who access investments in this area. It has only now become both technically and economically feasible to implement a common platform approach without writing off past investments in communication systems and equipment.

Advances in IP enable the ability to learn and turn knowledge into quick, decisive, and intelligent action, and are at the heart of successful organizations, systems, and societies. Public safety is no exception. A networked organization gathers and uses information much faster than a non-networked organization, and in the world of crisis management and homeland security, seconds count and can make the difference between success and failure. Taking a distributed network approach gives each organization infinite opportunities to define and implement new capabilities. These include the ability to detect and analyze relevant information where and when it is needed, share voice/radio communications efficiently, and improve response to crises as well as management of day-to-day operations.

It is important, too, that this approach focus on how information is organized and distributed rather than on how it is acquired. An enormous amount of information already exists within and flows through political and civil organizations. The challenge, therefore, lies in the ability to manage, coordinate, control, and communicate information already available. A distributed network platform provides great value in connecting the following elements:

· **Right information.** Major decisions about which information is "right" often compromise local needs and knowledge. Too much information is as bad as too little. The distributed network's ability to empower people at the edge of the network to gather the information they need in a standardized environment is critical, and goes a long way toward avoiding the trap of centralizing knowledge.

· **Right place, right person.** Only authorized individuals should have certain privileges for access to information and responsibilities for command-and-control operations.

· **Right time.** As a situation changes, the network platform provides the capability to self-synchronize and provide information instantaneously.

Resolving the Paradox

A distributed environment using Internet technologies provides remarkable, new opportunities for government and citizen interaction and involvement. It also creates a paradox: the actions of citizens and, regretfully, of our adversaries are moving faster than governments' abilities to keep up. Technology alone won't solve this challenge. It takes cooperation among governments, stakeholders, agencies, and others. Knowledge and the power to act, therefore, must move to the edge of the organization, away from centralized control.

It is also vital to have a coordinated plan and to forge agreements with all stakeholders at national, state, and local levels. Articulating this principle is one thing; putting it into practice is another. It is increasingly clear that barriers must be overcome to connect pockets of knowledge and achieve the flexibility and breadth required to strengthen our communities. Protecting public safeguards and ensuring public trust are issues much larger than any individual or organization. Using a distributed network platform for collaboration and cooperating in tandem creates a net effect—the wisdom of the crowd. A network, if empowered by the right people at the periphery, is far more effective at anticipating and solving problems than a single source. Essentially, the sum of a number of people is infinitely smarter than a single person. Now that we have a roadmap, it is time to take action.

More Information

The Cisco Internet Business Solutions Group (IBSG), the global strategic consulting arm of Cisco, helps Global Fortune 500 companies and public organizations transform the way they do business—first by designing innovative business processes, and then by integrating advanced technologies into visionary roadmaps that improve customer experience and revenue growth.

For further information about IBSG, visit http://www.cisco.com/go/ibsg

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

C11-410744-00 0707